REMARKS

Applicants have carefully studied the outstanding Official Action. The present amendment is intended to be fully responsive to all points of rejection and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the present application are hereby respectfully requested.

Claims 1, 33 and 38 stand rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicants regard as the invention. The Examiner states: "Claims 1, 33 and 38 recite the limitation 'the communication network' in lines 11, 12 and 12 respectively. There is insufficient antecedent basis for this limitation in the claims."

Applicants respectfully point out that claims 1, 33 and 38 all recite, in their respective preambles, "a communication network." Applicants therefore respectfully ask the Examiner to withdraw the 35 USC 112 rejection of claims 1, 33 and 38.

Claims 1 - 3, 5 - 6, 9 - 10, 12, 15 - 16, 33, 36, 38, and 40 stand rejected under 35 USC 103 as being unpatentable over US Patent 6,385,729 to DiGiorgio et al., in view of US Patent 6,044,349 to Tolopka et al.

Claims 4, 7 and 8 stand rejected under 35 USC 103 as being unpatentable over DiGiorgio et al., in view of Tolopka et al., and further in view of US Patent 6,055,637 to Hudson et al.

DiGiorgio et al. describes a secure token device which provides a user with a vehicle for accessing services that are provided by an Internet Service Provider (ISP). The user places the token device in communication with a reader that is coupled to a computer system. The computer system includes a web browser for accessing the services provided by the ISP. The token device may perform an authentication protocol to authenticate itself to the ISP. The ISP may also be required to authenticate itself. The token device may hold an electronic currency token for payment of services rendered by the ISP. The token device may contain stored personal information about the user. The user may stipulate

what portions of this personal information are provided to the ISP upon request. Contextual information regarding sessions with the ISP may also be stored on the token device and used to restore a context of a previous session during a subsequent session.

Tolopka et al. describes a portable storage medium used to store data and provide access to information from an information dissemination system (IDS). The storage medium can store one or more location/key pairs. Each of the location/key pairs designates a particular IDS location as well as an access key to the particular IDS location. The storage medium can also store a plurality of information units. Levels of information categories can be individually accessed and categories of information units within levels can selectively be downloaded.

Hudson et al. describes a resource access control system for an enterprise including a security administrator in communication with a plurality of users, each of the users having an assigned role and a unique identifier. A temporary credential token is generated with respect to the assigned role of the user by the security administrator as the user logs on by entering the assigned unique user identifier and indicates a desire to access a resource. The temporary credential token is communicated to the resource and any subsequent resources to allow access by the user, and deleted as the user terminates the session.

Claim 1 has been amended by including the recitation of claim 4.

Claim 4 has been cancelled.

The Examiner takes the position that claim 1 is obvious in light of DiGiorgio et al. in view of Tolopka et al., and further that claim 4 is obvious in light of DiGiorgio et al. in view of Tolopka et al., and further in light of Hudson et al..

Applicants respectfully point out that the prior art of record does not provide a suggestion to combine DiGiorgio et al., with Tolopka et al. and with Hudson et al..

Applicants further respectfully submits that the motivation to combine DiGiorgio et al., with Tolopka et al. and with Hudson et al. suggested by the Examiner is based on hindsight. None of the references provided by the Examiner provide said motivation.

Even assuming, for the sake of argument, contrary to the position of Applicants, that a combination of DiGiorgio et al., with Tolopka et al. and with Hudson et al. would be proper, the Examiner has failed to make a prima facie case of unpatentability against claim 4 because the combination of DiGiorgio et al., with Tolopka et al. and with Hudson et al. lacks certain features recited in claim 4.

More specifically, for example, Hudson et al. describes the use of a local administrator and the step of identifying the local administrator and determining the local administrator as a proxy administrator (col. 4, lines 50 - 58).

By contrast, amended claim 1 recites: "determining the local administrator as a proxy administrator for administrating said at least one smart card **by transmitting at least authorization information from the remote administrator to the local administrator.**" Hudson et al. does not describe or suggest transmitting authorization information from local security administrator 62 to the central security administrator 60; nor does the other prior art of record describe or suggest such a feature.

Amended claim 1 is therefore deemed allowable.

Claims 2, 3, 5 - 10, 12, and 15 - 16 depend either directly or indirectly from claim 1 and recite additional patentable subject matter.

Claims 2, 3, 5 - 10, 12, and 15 - 16 are therefore deemed allowable.

Claim 33 is a system claim corresponding to claim 1 and has been correspondingly amended.

Amended claim 33 is therefore deemed allowable.

Claim 36 depends from claim 33 and recites additional patentable subject matter.

Claims 36 is therefore deemed allowable.

Claim 38 is a means plus function claim corresponding to claim 1 and has been correspondingly amended.

Amended claim 38 is therefore deemed allowable.

Claim 40 depends from claim 38 and recites additional patentable subject matter.

Claim 40 is therefore deemed allowable.

Claims 11, 18, 35, 37, 39 and 41 stand rejected under 35 USC 103 as being unpatentable over DiGiorgio et al., in view of Tolopka et al., and further in view of US Patent 6,266,744 to Murphy et al.

Murphy et al. describes a method for authenticating a user over a network. The method includes an authentication module retrieving "authentication information from database 26." and storing in a smart card database at a remote location authentication information "by the same CA (Certified Authority) that issued the smart card to the user." (col. 6, lines 33 - 39).

Claims 11 and 18 depend from amended claim 1, and recite additional patentable subject matter.

Claims 11 and 18 are therefore deemed allowable.

Claims 35 and 37 depend, either directly or indirectly, from amended claim 33, and recite additional patentable subject matter.

Claims 35 and 37 are therefore deemed allowable.

Claims 39 and 41 depend, either directly or indirectly, from amended claim 38, and recite additional patentable subject matter.

Claims 39 and 41 are therefore deemed allowable.

In order to make the distinction of the claimed invention over Murphy et al., in light of DiGiorgio et al. and Tolopka et al. particularly clear, new dependent claims 42 and 43 have been added. New claims 42 and 43 are supported, intra-alia, by the discussion in the disclosure of the remote administrator which preferably performs authentication, verification and validation of the smart card "by using well known techniques of challenge-response of either information related to shared secrets or public/private keys, such as the RSA challenge-response scheme, the Fiat-Shamir identification and authentication scheme, and keyed-hash schemes" (pg. 15, line 30 - pg. 16, line 4).

Despite having overcome the rejection of claims 11, 18, 35, 37, 39 and 41, based on the argument above, for the sake of argument, Applicants wish to respond to the Examiner's rejection of 11, 18, 35, 37, 39 and 41. Claim 11 recites "the step of identifying the at least one smart card in a smart card data base at the remote administrator". Claim 18 recites that the "remote administrator comprises a plurality of administrators, each operative to perform at least one of the

following: at least part of said step of accessing the protected information resource; and at least part of an administration initialization procedure".

Claims 35 and 37 are system claims corresponding to the methods claimed in claims 11 and 18 respectively.

Claims 39 and 41 are means plus function claims corresponding to the methods claimed in claims 11 and 18 respectively.

Murphy et al., as discussed above, utilizes retrieval of authentication information from a database, thereby teaching away from the invention as claimed in claims 11, 18, 35, 37, 39 and 41.

The Examiner rejected claims 11, 35 and 39 as "it would have been obvious to one skilled in the art at the time the invention was made to modify the system of DiGiorgio et al. and Tolopka et al. to include a smart card database at the remote administrator and the step of identifying the smart card in a smart card database, as taught by Murphy et al., so that identification of smart cards can be easily stored and utilized by the remote administrator." It is respectfully submitted that the prior art cited by the Examiner does not suggest a motivation for combining the references, and thus including a smart card database at the remote administrator and the step of identifying the smart card in a smart card database. The Examiner is respectfully asked to provide such a reference and to supply such a motivation.

The Examiner rejected claims 18, 37 and 41 as, "it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of DiGiorgio et al. and Tolopka et al. such that the remote administrator comprises a plurality of administrator[s], as taught by Murphy et al., to have a flexible implementation of the remote administrator." It is respectfully submitted that the prior art cited by the Examiner does not suggest a motivation for combining the references, and thus utilizing a plurality of administrators. The Examiner is respectfully asked to provide such a reference and to supply such a motivation.

Claims 13 and 14 stand rejected under 35 USC 103 as being unpatentable over DiGiorgio et al., in view of Tolopka et al., and further in view of US Patent 5,943,423 to Muftic et al. Muftic et al. describes "a method of obtaining

access to computer or network resources using a smart token, comprising: opening an application domain of a smart token used for access to a computer or a network; encrypting a password read from the application domain, so as to obtain an electronic password; sending a logon identification and the encrypted password to the computer or network for which access is desired; and verifying and validating as to whether the logon identification and the encrypted password are such that the access to the computer or network is permitted, wherein the step of sending a logon identification to the computer or network for which access is desired comprises: sending a user public key certificate stored on the smart token together with a user identification and a user random number to the computer or network; receiving from the computer or network the identity of the computer or network, a public key certificate of a target resource, a signed copy of the user random number and a second random number generated by the computer or network; verifying the signed copy of the user random number; and signing the second random number using the public key of the computer or network obtained from a certificate and returning the second random number with signature to the computer or network" (claim 1).

Claims 13 and 14 depend indirectly from amended claim 1, and recite additional patentable subject matter.

Claims 13 and 14 are therefore deemed allowable.

Additionally, it is respectfully pointed out to the Examiner that the administration operations listed in claim 14 include several elements not disclosed by Muftic et al., including: "...renewal of said at least one smart card; expiration date updating; renewal of an authorization to said at least one smart card; validity check of data in said at least one smart card; integrity check of data in said at least one smart card; memory load/check; revocation of at least one of an authorization, a certificate and a smart card; execution of a "KILL CARD" process after a verification of a need to prevent operation of said at least one smart card; data load; and transmission of smart card chaining information"

Furthermore, the Examiner rejected claims 13 and 14 as "it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of DiGiorgio et al. and Tolopka et al. to include the

step of performing an administration operation by transmitting a certificate and credentials, as taught by Muftic et al., in order for the remote administrator to be able to control access to the protected resources." It is respectfully submitted that the prior art cited by the Examiner does not suggest a motivation for combining the references, and thus utilizing the step of performing an administration operation by transmitting a certificate and credentials to modify method of DiGiorgio et al. and Tolopka et al.. The Examiner is respectfully asked to provide such a reference and to supply such a motivation.

Claim 17 stands rejected under 35 USC 103 as being unpatentable over DiGiorgio et al., in view of Tolopka et al., and further in view of US Patent 5,838,812 to Pare, Jr. et al. Pare, Jr. et al. describes "a tokenless identification system and method for authorization of transactions and transmissions is described. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously. The method and apparatus can be networked to act as a full or partial intermediary between other independent computer systems, or may be the sole computer systems carrying out all necessary executions." In the system of Pare, Jr. et al., "when the computer system completes an operation, such as a registration of a buyer or a seller, or a particular transaction succeeds or fails, a presentation step **provides the results of the operation to the buyer and/or the seller**" (col. 6, lines 48 - 51).

The present invention, by contrast, as claimed in claim 17, performs an operation, "wherein each operation performed during said accessing step by at least one of said remote administrator and said at least one smart card is performed only upon receipt of an 'END ADMINISTRATION OPERATION' instruction at a corresponding one of said at least one of said remote administrator and said at least one smart card". Thus, the 'END ADMINISTRATION OPERATION' instruction is specific to the remote administrator, and only following such a message can further operations be performed. There is no recitation of a message being sent to an end user.

The Examiner rejected claim 17 as, "it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of DiGiorgio et al. and Tolopka et al. to present a message at the end of an administrative procedure, as taught by Pare, Jr. et al., so that users can be informed of the result of the operation. It is respectfully submitted that the prior art cited by the Examiner does not suggest a motivation for modifying the method of DiGiorgio et al. and Tolopka et al. to present a message at the end of an administrative procedure. The Examiner is respectfully asked to provide such a reference and to supply such a motivation.

In any event, claim 17 depends indirectly from amended claim 1, and recites additional patentable subject matter.

Claim 17 is therefore deemed allowable.

Applicants have carefully studied the other prior art of record including US Patent 6,325,292 to Sehr (erroneously cited as Sher in the Office Action, but correctly named in the Examiner's Notice of References Cited). Sehr describes a card system and methods that encompass a card issuer entity and a plurality of service providers so as to automatically compile, issue, utilize, and process collector cards for the purpose of enjoyment, purchase of goods and services, and for the activation of other card-based privileges. The portable collector cards are realized by smart card technology and have the ability to compile and process collectible information, and store and use a monetary amount to simulate debit/credit card payment means. Applicants find that the present invention as claimed is neither described nor suggested in the prior art of record, taken either individually or in combination.

In view of the foregoing remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,

JULIAN COHEN
c/o LADAS & PARRY
26 WEST 61st STREET
NEW YORK, N. Y. 10023
Reg. No. 20302 (212) 708-1887